STATE OF ARIZONA
2006 INTERIM
STATE INFRASTRUCTURE
PROTECTION PLAN

Securing Arizona, Together

Frank Navarrete
Director

Janet Napolitano
Governor

Preface

The National Infrastructure Protection Plan (NIPP) does not address the specific needs of the state. However, because the crucial role the state to protect critical infrastructure in a way that aligns with the national vision, therefore the creation of the Interim State Infrastructure Protection Plan (SIPP) was created. A SIPP is vital for the security of Arizona in the event of a terrorist attack, natural disaster, or any other type of incident. The SIPP helps first responders ensure that Arizona's Critical Infrastructure/Key Resources (CI/KR) are kept safe, strong, and prosperous. This plan draws guiding principles and objectives from a variety of sources, including, but not limited to: *National Infrastructure Protection Plan, Homeland Security Presidential Directive (HSPD-7) and HSPD-8, State of Arizona 2006 Homeland Security Grant Program Enhancement Plan, Geospatial Antiterrorism Buffering, Response and Intervention System Providing Education and Logistical Support, and the Arizona Homeland Security Strategy.* For more information regarding Arizona Homeland Security documents please visit our website at: http://www.homelandsecurity.az.gov.

Introduction

Purpose

Fundamental to the mission of the U.S. Department of Homeland Security (DHS) is the mitigation of threats, vulnerabilities, and consequences that stem from acts of terrorism and other critical hazards. This is a shared responsibility and commitment of Federal, State, Tribal, and local governments, as well as the private sector. State, Tribal, and local governments are responsible for implementing the homeland security mission, protecting public safety and welfare, and ensuring the provision of essential services to communities and industries within their jurisdictions. The purpose of the SIPP is to provide strategic direction to these entities and reduce the risk of terrorist incidents.

Objective

Enhance protection of the State's CI/KR in order to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorist or other critical hazards to destroy, incapacitate, or exploit them; enable Arizona's preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency; and to prevent and protect the citizens of Arizona through proactive measures.

Threats

The Governor's guidance and state strategies focuses CI/KR efforts on addressing the emerging terrorist threat environment as an essential component of the all-hazards approach of the homeland security mission. The emergence of the terrorist threat as a reality in the 21st Century presents new challenges and requires new approaches focused on intelligence-driven analysis, information sharing, and unprecedented partnerships between the public and private sector. As a result of decades of experience responding to catastrophic/non-catastrophic natural disasters, industrial accidents, and the deliberate acts of malicious individuals, the State's CI/KR are generally resilient. However, government and business contingency, incident, and emergency response plans and preparedness efforts must now also address the unique aspects of the terrorist threat and other critical hazards.

These unique aspects are addressed by:

- Direct Infrastructure Effects;
- Indirect Infrastructure Effects;
- Exploitation of Infrastructure

The following qualify as a terrorist threat or state significant disaster:

- Causes catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;
- Impairs State departments and agencies' abilities to perform essential missions, or to ensure the public health and safety;
- Undermines State and local government capacities to maintain order and to deliver minimum essential public services;
- Damages the private sector's capability to ensure the orderly functioning of the economy and delivery of essential service;
- Has a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources;

- Undermines the public’s morale and confidence in our national economic and political institutions.

Roles and Responsibilities

As defined by the NIPP, these separate authorities are tied together as part of the national approach for CI/KR protection through the unifying framework established in HSPD-7. HSPD-7, issued in December 2003, established the U.S. policy for "enhancing protection of the Nation's CI/KR." Given that terrorist incidents and certain natural or man-made disasters will have a statewide impact, it is vital that Arizona's government provides overarching leadership to Tribal and local governments and coordination in the CI/KR protection mission area. The following sections address the security partner roles and responsibilities under this integrated approach.

Arizona Department of Homeland Security-As defined by HSPD-7 and the NIPP:

Under the HSPD-7 framework, Arizona Department of Homeland Security (ADOHS) is responsible for leading, integrating, and coordinating the overall statewide effort to enhance CI/KR protection, including developing the SIPP; developing and implementing comprehensive multi-tiered risk-reduction programs and methodologies; developing cross-sector and cross-jurisdictional protection guidance, guidelines, and protocols; and establishing risk management and performance criteria and metrics within and across sectors.

Additional duties include:

- Establish a 24/7 intelligence/information analysis center that will serve as the central hub to facilitate the collection, analysis and dissemination of crime and terrorism related information in Arizona;
- Coordinate between the State agencies, Tribes, regions, and private sectors to ensure that all are effectively communicating and following the same guidelines;
- Collaborate with Mexico to strengthen the protection and security of Arizona's borders;
- Maintain open communication with neighboring states in order to enhance Arizona's information and intelligence resources;
- Facilitate the sharing of CI/KR protection best practices and processes, as well as risk assessment methodologies and tools across sectors and jurisdictions;
- Maintain a State budget and inform the regions and Tribes of what they are allocated;
- Allocate resources for CI/KR based on risk and need;
- Address unique geographical issues, including trans-border concerns, dependencies, and interdependencies among the sectors within the jurisdiction.

State-As defined by HSPD-7 and the NIPP:

The Arizona government is responsible for establishing security partnerships, facilitating coordinated information sharing, and enabling planning and preparedness for CI/KR protection within it's jurisdictions. Arizona serves as a crucial coordination hub, bringing together prevention, protection, preparedness, and response authorities, capacities, and resources among local, Tribal jurisdictions, across regional entities and the state. The state will also act as conduits for requests for Federal assistance when the threat situation or current incident exceeds the capabilities of public and private sector security partners at lower jurisdictional levels. State departments and agencies shall implement this directive in a manner consistent with applicable provisions of law, including those protecting the rights of citizens of the United States.

Arizona government will:

- State departments and agencies will identify, prioritize and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. State departments and agencies will work with the Federal, Tribal, local governments and the private sector to accomplish this objective;
- State departments and agencies will ensure that homeland security programs do not diminish the overall economic security of Arizona;
- State departments and agencies will appropriately protect information associated with carrying out this directive, including handling voluntarily provided information that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the Homeland Security Act of 2002.

Local Government-As defined by HSPD-7 and the NIPP:

Local governments are the first line of defense. They see first hand the changes that occur in their respective areas. They will be the first to notice any anomalies, and the first to respond to an incident and decrease the impact of the event.

Local governments will:

- Provide information to the Arizona Counter Terrorism Information Center's (AcTIC) Threat and Vulnerability Assessment (TVA) team on CI/KR deemed critical from the local level to enable prioritized protection and restoration of critical public services, facilities, utilities, and processes within the jurisdiction;
- Ensure that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the CI/KR protection mission in accordance with relevant plans and strategies;
- Address unique geographical issues, including trans-border concerns, dependencies, and interdependencies among agencies and enterprises within the jurisdiction;
- With assistance of the TVA team conduct or facilitate vulnerability assessments of their areas;
- Encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources;
- Act as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local agencies, businesses, and citizens;
- It is suggested to conduct bi-annual Table Top exercises that maintain the readiness of their first responders.

Tribal-As defined by HSPD-7 and the NIPP:

Arizona Department of Homeland Security recognizes the sovereignty of the Tribes and the integral part they play in achieving the State's HS strategy. Tribal governments are ultimately accountable for the public health, welfare, and safety of Tribal members, as well as the protection of CI/KR and continuity of essential services under their jurisdiction.

Tribal Government will:

- Ensure that all CI/KR are identified to include sacred sites, lands, burial sites, waters, and mountains;
- Work with and maintain open communications with local, state, federal agencies, and surrounding regions;
- Maintain a real time information link between AcTIC, state and federal law enforcement and first responder agencies;
- Work with the Arizona Threat and Vulnerability Assessment team (TVA) to concentrate the effort of acquiring site data and guiding the application of protective measures.

Private Sector, Other Owners and Operators:

Owners and operators generally represent the first line of defense for the CI/KR under their control. Owners and operators are responsible for taking action to support risk management planning and investment security as a necessary component of prudent business planning and operations. In today's risk environment, these activities generally include reassessing and adjusting continuity-of-operations and emergency management plans, building in increased resiliency and redundancy into business processes and systems, hardening facilities against the physical and cyber attacks and natural disasters, and increased coordination with external organizations to avoid or minimize the impacts on surrounding communities or industry partners.

Private security agencies are in many cases the first line of defense. The AcTIC is developing a partnership with private agencies. It is vital that private sectors and sector-specific agencies collaborate on security issues and maintain open lines of communication. The Interim SIPP defines key resources to include dams, government facilities, commercial facilities, nuclear reactors, materials, and waste.

Sector-Specific Agencies

Recognizing that each CI/KR sector possesses its own unique characteristics, operating models, and risk landscape, HSPD-7 designates Federal government Sector-Specific Agencies (SSA) for each of the 17 CI/KR sectors. At the sector level, SSAs are responsible for working with DHS to implement the NIPP sector partnership model and risk management framework, develop protective programs and related requirements, and provide CI/KR protection guidance in line with overarching guidance established by DHS pursuant to HSPD-7. Working in collaboration with security partners, they are responsible for developing and submitting Sector Specific Plan (SSP) and sector-level performance feedback to DHS to enable national-level gap assessments.

Sector-Specific Agencies and HSPD-7 Assigned CI/KR Sectors are:

Department of Agriculture
Agriculture, food (meat, poultry, egg products)-AZ Department of Agriculture

Department of Health and Human Services
Public health and healthcare-AZ Department of Health Services

Food (other than meat, poultry, egg products)-AZ Department of Commerce

Environmental Protection Agency
Drinking water and wastewater treatment systems-AZ Water Resources

Department of Energy
Energy, including the production, refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities)-AZ Corporation Commission

Department of the Treasury
Banking and finance- Banking

Department of the Interior
National monuments and icons-Parks and Services

Department of Defense
Defense industrial base-Emergency and Military Affairs

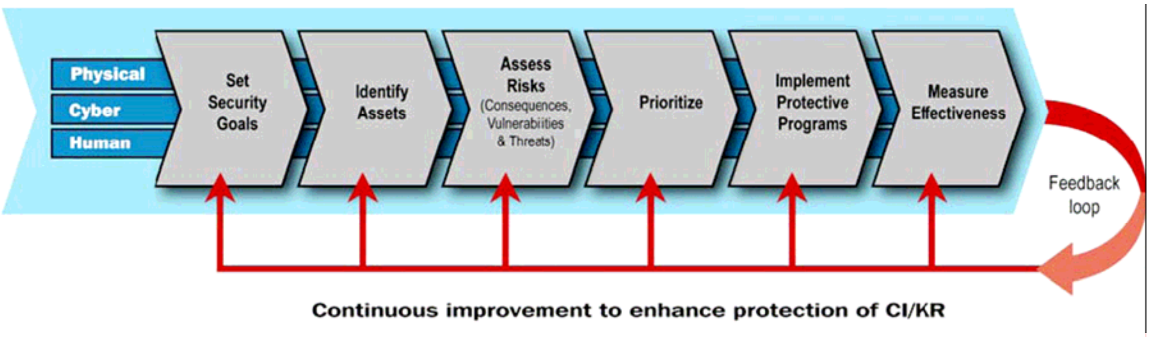
Department of Homeland Security
Chemical (DHS/IP)-Environmental Quality
Commercial facilities (DHS/IP)-Individual Agencies
Dams (DHS/IP)-U.S. Bureau or Reclamations
Emergency services (DHS/IP)
Commercial nuclear reactors, materials, and waste (DHS/IP)-AZ Radiological Regulatory Association
Information technology (DHS/Cyber and Telecommunications Security)-GITA
Telecommunications (DHS/Cyber and Telecommunications Security)-AZ Corporation Commission
Postal and shipping (DHS/TSA)- U.S. Postal Services
Transportation systems (DHS/TSA, USCG6)-Transportation
Government facilities (DHS/FPS)- State Government

The duties of Sector-Specific Agencies (SSA) and Private Sectors will include:

- Perform comprehensive risk assessments tailored to their specific sector, enterprise, or facility risk landscape;
- Implement protective actions and programs to reduce identified vulnerabilities appropriate to the level of risk presented;
- Assist and support Federal, State, Tribal and local government CI/KR protection efforts, as appropriate;
- Collaborate with all relevant Federal and State departments and agencies; Tribal and local governments, and the private sector, including with key persons and entities in their infrastructure sector;
- Conduct or facilitate vulnerability assessments of the sector;
- Encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

Protection Program Strategy

The physical, cyber, and human elements of the CI/KR are considered during each step of the risk management framework. The SIPP risk management framework includes the following steps: set security goals, identify assets, assess risks, prioritize, implement protective programs, measure effectiveness, and a feedback that loops back through the entire program.


Physical
Cyber
Human
Set Security Goals
Identify Assets
Assess Risks (Consequences, Vulnerabilities & Threats)
Prioritize
Implement Protective Programs
Measure Effectiveness
Feedback loop
Continuous improvement to enhance protection of CI/KR

Source: NIPP, under Protection Program Strategy

Set Security Goals

Achieving a secure, protected, and resilient infrastructure requires statewide and sector-specific security goals that collectively represent the desired security posture. These goals should consider the physical, cyber, and human elements of CI/KR protection.

Arizona’s priority goals include:

- Ensuring that first responders have access to personal protective equipment;
- Improve communication system to allow first responders to communicate with one another during emergencies;
- Bolster security in the state, especially at the border and at sites with critical infrastructure;
- Improve overall detection and response capabilities.

Identify Assets

Once the security goals are set, the next step is to identify assets. To do this, a comprehensive inventory of the State’s infrastructure must be developed and maintained. CI/KR priorities may change quickly based on numerous factors, including the dynamic nature of the terrorist threat, evolving technologies, the economy, or damages resulting from any other critical hazard. In order to appropriately manage risk in real time, Arizona is required to maintain a comprehensive and up-to-date inventory that includes certain basic information on the assets, systems, and networks that comprise Arizona's CI/KR.

Risks

A variety of methodologies are available to facilitate comprehensive risk assessment that integrate and disseminate information throughout partnering government agencies. These are mainly through the Arizona Threat and Vulnerability Assessment (TVA), GABRIEL, and AcTIC.

The three following factors are combined to define risk:

- **Consequence-** the range of loss or damage that can be expected from a successful attack;
- **Vulnerability**- The characteristic of, or flaw in an asset, system or network's design, location, security posture, or operations that renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards; and
- **Threat-** The likelihood that a particular target, or type of target, will suffer an attack or incident. In the context of risk from terrorist attack, threat likelihood is based on the analysis of the intent and the capability of an adversary.

Risk assessment is a comprehensive systematic approach to identify CI/KR. Risks have to be assessed beyond the immediate asset to include it's systems and networks. To determine risk, consequences, vulnerabilities, and threats associated with the asset, system, or network; risks are assessed and combined. The risk assessment may require expansion geographically to sectors, regions and/or the state and can be calculated for an asset, system, or network by sector, region, or state. The result is a comprehensive, systematic assessment of asset, system, sector, regional, or state risk that informs integrated risk-reduction activities.

Consequence Analysis is the result of a terrorist attack or other incident that reflects the level, duration, and nature of the loss resulting from the incident. For the purpose of the SIPP, these consequences are divided into four main categories.

These four categories are:

- **Health Impact-** Effect on human life and physical well-being (e.g., fatalities, injuries);
- **Economic Impact-** Direct and indirect effects on the economy (e.g., cost to rebuild asset, cost to respond to and recover from attack, downstream costs resulting from unavailability of product or service);
- **Psychological Impact-** Effect on the public's morale and confidence in national economic and political institutions;
- **Governance Impact-** Effect on the government's ability to maintain order, deliver minimum essential public services, ensure the public's health and safety, and carry out national security-related missions.

Threat is an indication of possible violence, harm, or danger that includes both intent and capabilities. In the context of the SIPP, a threat is the likelihood that a particular target, or type of target, will suffer an attack or incident; for terrorist attack, threat likelihood is based on the analysis of the intent and capability of an adversary.

Geospatial Antiterrorism Buffering, Response and Intervention System Providing Education and Logistical Support- GABRIEL

The Arizona Infrastructure Protection Program is a component of an entire protection system, managed by the Terrorism Liaison Officers (TLO) Program, and is contained under one project umbrella: GABRIEL. GABRIEL has provided a flexible system to organize and combine the efforts from Federal, State, County, Tribal and Local Law Enforcement representatives, Fire Personnel, State Planners, FBI, DHS, National Guard representatives and regional government representatives into a unified system to compile data and critical information on sites that are identified as potential targets of terrorism. The Automated Critical Asset Management Systems (ACAMS) will ultimately serve as the data organization system that will assist the program participants in this process. Program data complies with National Protected Critical Infrastructure Information Program (PCII) Standards and Protocols. The Arizona Threat and Vulnerability Assessment (TVA) Program coordinates and collaborates the acquisition of data and the application of protective measures at CI/KR locations throughout the state of Arizona. Team members represent interests inside of the Urban Area Security Initiative (UASI) area as well as interests in the lesser concentrated metropolitan areas and rural locations. The Program coordinates efforts of program participants with the Phoenix TVA Program to insure consistency and collaboration in all areas of the program. The Arizona

Infrastructure Protection Program will manage the data system and administer PCII protocols through the TLO unit.

Prioritize

After risk-related data has been collected, combined, and analyzed, the results of the risk assessments are prioritized to help identify where risk reduction is most pressing, and to subsequently determine what protective action should be taken. Prioritization requires a comparison of the relative levels of asset and sector risk along with options for achieving the established security goals.

Implement Protective Programs

Protection is actions to guard or shield CI/KR assets, systems, networks, or their interconnecting links from exposure, injury, destruction, incapacitation, or exploitation. In the context of the SIPP, protection includes actions to deter, mitigate, or neutralize the threat, vulnerability, or consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, including hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, and implementing strict security measures.

Protective actions attempt to indirectly affect the threat and directly affect vulnerability and consequence as follows:

- **Deter**-Cause the potential attacker to perceive that the risk of failure is greater than that which they find acceptable;
- **Devalue**-Reduce the attacker's incentive by reducing the target's value.
- **Detect-**Identify potential attacks and validate and/or communicate the information, as appropriate;
- **Defend**-Protect assets by preventing or delaying the actual attack, or reducing an attack's effect on an asset.

Protective programs also may include actions that have an impact on the consequences should attack occur. These actions are focused on the following aspects of preparedness:

- **Mitigate**- Lessen the potential impacts of an attack, such as introducing system redundancy and resiliency, reducing asset dependency, or isolating downstream assets;
- **Respond**- Design to enable rapid reaction and emergency response to an attack, such as conditioning exercises and having adequate crisis response plans, training, and equipment; and

- **Recover-** Allow the sector to resume operations quickly and efficiently, such as developing the continuity-of-operations plans.

Characteristics of effective CI/KR protective programs, include, but are not limited to the following:

- **Comprehensive-** Effective protective programs must address the physical, cyber, and human elements of CI/KR, as appropriate, and consider long-term, short-term, and sustainable activities;
- **Coordinated**-Because of the highly distributed and complex nature of CI/KR sectors, the responsibility for protecting assets must be coordinated.
- **Cost-Effective-** Effective protective programs seek to use resources efficiently by focusing on protective actions that offer the greatest reduction in risk for any given expenditure;
- **Risk-Based**-Protective programs focus on reducing risk by affecting the elements of risk, individually or collectively. Protective actions should be designed to allow measurement, evaluation, and feedback based on risk reduction.

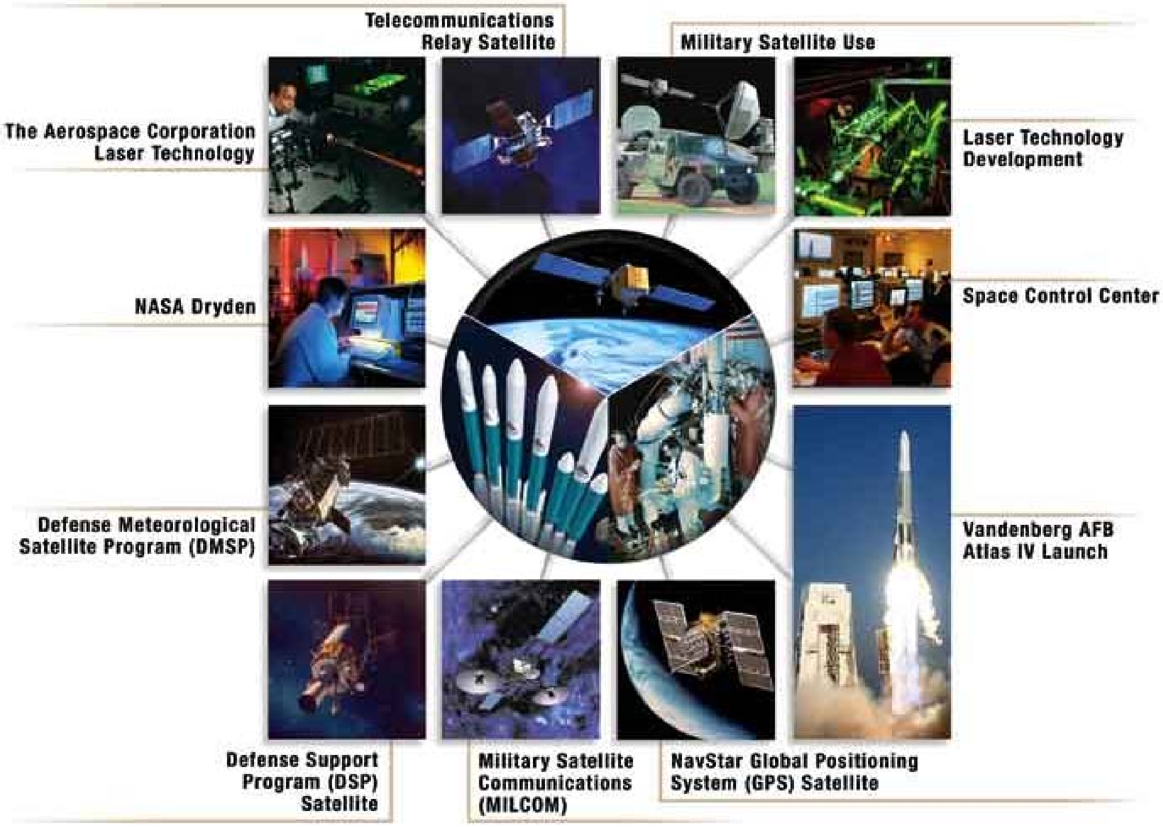
Protective Programs, Initiatives, and Reports

ADOHS/AcTIC, in collaboration with other security partners, undertakes a number of protective programs, initiatives, activities, and reports that support CI/KR protection. Many of these are available to provide resources to security partners. These activities span a wide range of efforts, including:

- **Buffer Zone Protection Program (BZPP)-** Grant program designed to provide resources to State and local law enforcement to enhance security "outside the fence";
- **Site Assistance Visits (SAVs)-** Facility security assessments designed to facilitate vulnerability identification and mitigation discussions between the Federal government and individual owners and operators;
- **Government Forum of Incident Response and Security Teams**- Facilitates interagency information sharing for cyber system protection;
- Geospatial Antiterrorism Buffering, Response and Intervention system providing Education and Logistical support (GABRIEL);
- Protected Critical Infrastructure Information (PCII); and
- Arizona Threat and Vulnerability Assessment (TVA).

Measure Effectiveness

Measuring effectiveness drives continuous improvement of CI/KR protective actions and programs at the sector level and overall program performance at the state and national levels. The SIPP uses a metrics-based system to provide feedback on efforts to attain the goals and objectives. The metrics also provide a basis for establishing accountability, documenting actual performance, facilitating diagnoses, promoting effective management, and reassessing goals and objectives. Metrics offer a quantitative assessment to affirm that specific objectives are being met or to articulate gaps in the state effort. They enable identification of corrective actions and provide decision makers with a feedback mechanism to help them make appropriate adjustments. Lessons learned from exercises and actual incidents and alerts provide additional objective input into the process.


Telecommunications Relay Satellite
Military Satellite Use
The Aerospace Corporation Laser Technology
Laser Technology Development
NASA Dryden
Space Control Center
Defense Meteorological Satellite Program (DMSP)
Vandenberg AFB Atlas IV Launch
Defense Support Program (DSP) Satellite
Military Satellite Communications (MILCOM)
NavStar Global Positioning System (GPS) Satellite

Organization for CI/KR Protection

Arizona was one of the first states to develop a regional approach to homeland security. The U.S. Department of Homeland Security has highlighted regionalization as a "vital step" in the state homeland security efforts.

Arizona is divided into five regions with a Regional Advisory Council (RAC) established to represent each region. The RACs are comprised of first responders and local elected officials that live or work in these regions, including: two members from fire service (one rural, one urban); one police chief; one sheriff; one member from Tribal government; one emergency manager; one mayor; one county supervisor; two at large members from the public and private sector; and an ad hoc member from both the Arizona Department of Public Safety and county public health. It is through these RACs, which meet at least four times a year, that homeland security projects are initially selected, submitted, and prioritized.

Cyber Security

ADOHS uses strict information security protocols for the access, use, and storage of sensitive information including that related to CI/KR. These protocols include both physical security measures and cyber security measures. Information security protocols include access controls, login restrictions, session tracking, and data labeling.

Under the SIPP, risk management follows a logical process that is comprised of the following fundamental activities:

- Setting security goals;
- Identifying assets, including cyber assets, systems, and networks;
- Assessing risk, which is based on consequences, threats, and vulnerability;
- Prioritizing efforts that will make the greatest reduction in risk;
- Implementing programs; and
- Measuring effectiveness and improving programs.

Arizona Counter Terrorism Information Center –AcTIC

AcTIC is the interagency intelligence operation that is the centerpiece of Arizona's Homeland Security detection and prevention strategy. It has a total of 34 agencies; 22 state and local and 12 federal. AcTIC has over 200 agents. It was built on the existing criminal intelligence systems within Arizona. AcTIC is responsible for integration of the other intelligence/information sources, and develops and implements fusion links and processes. Its capabilities are full cycle intelligence operations: collect, analyze, disseminate- Arizona and regional focus. They are a 24/7 operation with accessibility to the general public as well as homeland security actors, enhancing all sources of analysis. AcTIC provides multiple services including an Intel training center, a real time Intel analysis faculty for state leaders, a data warehouse, and emergency power and data recovery systems.

Information Sharing

Information sharing is both a critical component and a net result of establishing effective security partnerships. When owners and operators are provided with a comprehensive picture of threats and participate in ongoing two-way information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced. Similarly, when government is equipped with a solid understanding of private sector information needs and requirements, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

Homeland Security Information Network

Homeland Security Information Network (HSIN) is computer web-based counter terrorism communications system, distributed to all 50 states to strengthen the flow of threat information. HSIN's communications capability delivers real-time interactive connectivity with the DHS Homeland Security Operations Center, at the Sensitive-but-Unclassified (SBU) level to all users immediately. The HSIN system is DHS's primary means to distribute intelligence information and threat situational awareness. The HSIN can be utilized by security partners to obtain, analyze, and share information.

Law Enforcement Online

Law Enforcement Online (LEO) is a virtual private network provided by the FBI to all levels of the law enforcement, criminal justice, and public safety communities and is an "anytime and anywhere" system for secure electronic communications, online training, and information sharing. The LEO system is a state-of-the-art internet system that is approved by the FBI for sensitive but unclassified law enforcement sensitive information. Accordingly, LEO is used to support investigative operations, send notifications and alerts, and provide an avenue for a single sign-on to remotely access other law enforcement and intelligence systems and resources.

Memorandum of Understanding

In March 2006, Governor Napolitano signed a Memorandum of Understanding (MOU) with California, New Mexico and Texas. This MOU would permit the four state intelligence fusion centers, AcTIC, California State Terrorist Threat Assessment Center - STTAC, the New Mexico Office of Homeland Security, and the Texas Fusion Center - TFC, to share unclassified and when necessary classified intelligence to better provide homeland security. The four centers will conduct at a minimum one joint exercise per year to assure that intelligence is being quickly and effectively shared. The previous MOU was only with New Mexico and did not include classified information. The current MOU is vital to maintaining homeland security for the southwest region. The shared border between the four states lends a common challenge as it relates to homeland security.

Protected Critical Infrastructure Information and Other Security Regimes

The Protected Critical Infrastructure Information (PCII) Program was established pursuant to the Critical Infrastructure Information (CII) Act of 2002. The Program provides a means for sharing private sector information with the government while providing assurances that the information will be exempt from unauthorized public disclosure and will be properly safeguarded. This enables members of the private sector to voluntarily submit sensitive information regarding the CI/KR to DHS with the assurance that the information will be protected.

DHS established the PCII Program Office to manage CII information, develop protocols for handling this information, and raising awareness of the need for protected information sharing between the public and private sectors. The PCII Program Office is responsible for receiving, validating, and safeguarding CII submitted to DHS. The Program Office works with government programs and those entities in the private sector willing to share their information on a voluntary basis.

The Protective Security Advisor (PSA) Program is when DHS protection specialists are assigned as liaisons between DHS and the protective community at the state, local, and private sector levels representing major concentrations of CI/KR across the United States. The PSAs are responsible for sharing risk information and providing technical assistance to local law enforcement and the owners and operators of assets within those areas.

Leadership in Energy and Environmental Design- application as defined by GABRIEL

One of the objectives of the GABRIEL Program is to promote the establishment of accepted standards for Site Protection Systems that can be applied by Architects, Engineers and Designers in Arizona as they consider the most appropriate and practical methods for implementation of threat mitigation measures at specific locations. Currently there are no universal building codes or accepted design standards relating to security design or terrorism prevention measures that apply to across the board to all types of developments or retrofitting applications. The currently existing protective design standards that are applicable to newly constructed Governmental structures or leased properties under mandates that have been established by the General Services Administration (GSA) and the Department of Defense (DoD). There are also a number of agencies and organizations in existence that have formed and promoted their own protections programs and standards such as those utilized by the Federal Emergency

Management Agency (FEMA), the National Fire Protection Association (NFPA), the United States Air Force, the United States Army, the Department of State (DOS), the American Society for Industrial Security (ASIS) and the Center for Disease Control (CDC). However, the mandated application of protective design components or systems to civilian developments does not currently exist outside of jurisdictions that require the inclusion of Crime Prevention through Environmental Design methodology.

The Leadership in Energy and Environmental Design (LEED) Green Building Rating System is a voluntary, consensus-based national standard for developing "high-performance", sustainable buildings based upon the Whole Building Design Philosophy.

LEED was originally created by the Department of Energy to:

- Define "green building" by establishing a common standard of measurement;
- Promote integrated, whole-building design practices;
- Recognize environmental leadership in the building industry;
- Stimulate green competition;
- Raise consumer awareness of green building benefits.

LEED provides a complete framework for assessing building performance and meeting sustainability goals. Based on accepted scientific standards, LEED programs emphasize strategies for sustainable site development, water savings, energy efficiency, materials selection and indoor environmental quality. LEED is widely accepted by governing entities throughout the United States and recognizes achievements and promotes expertise through a comprehensive system offering project certification, professional accreditation, training and practical resources.

A further development in the expansion of the LEED system that merges Whole Building Design Concepts with ISC Design Standards and DOD Antiterrorism Standards has been accomplished by the implementation of the LEED-DoD Antiterrorism Standards Tool. The LEED-DoD Antiterrorism Standards Tool addresses the security implications of strategies used to achieve each LEED credit with regard to their inter-relationship (i.e., potential conflicts and synergies), from the Department of Defense (DoD) perspective. Information is presented within a color-coded matrix based on the U.S. Green Building Council's Leadership in Energy and Environmental Design Green Building Rating System.

Measures taken by the state:

- Arizona will start creating a standardized building plan for major structures within the state. Buildings or structures whose loss will endanger the public need to be identified by the accepted standard of ODP/DHS CI/KR sectors and necessary actions taken to ensure their safety;

- Existing high profile government and CI/KR buildings need to be updated to meet this standard, if they do not already.

- Promoting the acceptance and utilization of the LEED-DoD Antiterrorism Standards Tool by state, local and regional design review agencies throughout Arizona.

Arizona's CI/KR is widely distributed in both a physical and logical sense. Effective CI/KR protection requires both distributed implementation of protective programs by security partners, and centralized leadership to ensure implementation of a reasonable, comprehensive, coordinated, and cost effective approach that helps to reduce the risk to the State's infrastructure.

Awareness, Training, and Exercise Programs

It is suggested that Arizona hold an annual tabletop exercise that will test the state's preparedness in dealing with terrorist/natural disaster actions. Each year, the focus will be on a different sector, region or Tribe, and a variety of CI/KR.

As defined by the Interim National Preparedness Goal, the Target Capabilities List (TCL) provides guidance on the specific capabilities and levels of capability that State, Tribal, and local entities will be expected to develop and maintain. Every entity will not be expected to develop and maintain every capability to the same level. The specific capabilities and levels of capability will vary based upon the risk and needs of different types of entities; for example, basic capabilities and levels may be expected of individual jurisdictions and more advanced capabilities and levels may be expected of groups of jurisdictions or States.

While many capabilities are common to most, scenarios, conditions and performance standards for a capability can vary significantly. Full capabilities may take years to develop and maintain. National preparedness requires every entity to do their part to develop and maintain the appropriate capabilities and levels of capability that the State may need to draw upon in time of emergency.

Acronyms

ACAMS-Automated Critical Asset Management Systems
AcTIC-Arizona Counter Terrorism Information Center
BZPP-Buffer Zone Protection Program
CII- Critical Infrastructure Information
CI/KR- Critical Infrastructure and Key Resources
DHS- Department of Homeland Security
GABRIEL- Geospatial Antiterrorism Buffering, Response and Intervention System Providing Education and Logistical Support
HSIN- Homeland Security Information Network
LEED-Leadership in Energy and Environmental Design
LEO- Law Enforcement Online
MOU-Memorandum of Understanding
NIPP-National Infrastructure Protection Plan
OTM-Other Than Mexican
PCII-National Protected Critical Infrastructure Information Program
PSA- Protective Security Advisor
SAVs-Site Assistance Visits
SIPP-State Infrastructure Protection Plan
SSA- Sector-Specific Agencies
SSP- Sector-Specific Plan
STTAC-California State Terrorist Threat Assessment Center
TCL- Target Capabilities List
TFC-Texas Fusion Center
TLO-Terrorism Liaison Officers
TVA-Arizona Threat and Vulnerability Assessment
UASI-Urban Area Security Initiative

Glossary of Key Terms

All-Hazards. An approach for prevention, protection, preparedness, response, and recovery that addresses the full range of threats, including domestic terrorist attacks, natural and man-made disasters, and emergencies.

Asset. As defined in the Homeland Security Act of 2002, assets include contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).

Consequence. The result of a terrorist attack or other incident that reflects the level, duration, and nature of the loss resulting from the incident. For the purposes of the NIPP, these consequences are divided into four main categories:

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, networks, or functions would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Critical Infrastructure Information (CII). As defined by the Critical Infrastructure Information Act of 2002, CII includes information not customarily in the public domain and related to the security of critical infrastructure or protected systems.

Cyber security. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure the information's confidentiality, integrity, and availability.

Dependency. The one-directional reliance of an asset, sector, or sectors on other input, interaction, or other requirement in order to function properly.

Health Impact: Effect on human life and physical well-being (e.g., fatalities, injuries).

Economic Impact: Direct and indirect effects on the economy (e.g., cost to rebuild asset, cost to respond to and recover from attack, downstream costs resulting from unavailability of product or service).

Governance Impact: Effect on the government's ability to maintain order, deliver minimum essential public services, ensure the public's health and safety, and carry out national security-related missions.

Hazard. Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

Infrastructure. As defined in Executive Order 13010, infrastructure is the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition of assets in the Homeland Security Act, infrastructure assets include of one or more of the following elements:

- **Physical elements**: Tangible property such as facilities, components, real estate, animals, and products.
- **Cyber elements**: Electronic information and communications systems and the information contained in those systems. Information and communications systems are comprised of all the hardware and software that processes (i.e., creates, accesses, modifies, and destroys), stores (e.g., all media types: paper, magnetic, and electronic), and communicates (i.e., shares and distributes) information, or any combination of all of these elements.
- **Human elements**: Critical knowledge, expertise, or functions of people (i.e., tacit knowledge and job expertise or skills) uniquely susceptible to destruction, incapacitation, or exploitation through the individuals who possess or use such knowledge.

Interdependency. The reliance of an asset, sector, or sectors on other assets or sectors to function properly, and their reliance on the original entity in return. This reliance is reciprocal and, at a minimum, bidirectional.

Key Assets. Individual targets whose destruction could cause large-scale injury, death, or destruction of property, and/or profoundly damage national prestige, and confidence.

Key Resources. As defined in the Homeland Security Act of 2002, key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

Network. In the context of the SIPP, a network is a group of assets or systems that share information or interact with each other in order to provide infrastructure services to the Nation.

Normalize. In the context of the SIPP, to normalize is the process of transforming risk data into comparable units.

Preparedness. The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private sector and non-governmental organizations to identify threats, determine vulnerabilities, and identify required resources.

Prevention. Actions taken to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions taken to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; immunizations, isolation, or quarantine; public health and agricultural surveillance and testing processes; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Prioritize. In the context of the SIPP, to prioritize is the process of using risk assessment results to identify where risk-reduction efforts are most needed and subsequently determine which protective actions should be instituted in order to have the greatest effect.

Protection. Actions to guard or shield CI/KR assets, systems, networks, or their interconnecting links from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, protection includes actions to deter, mitigate, or neutralize the threat, vulnerability, or consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, including hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, and implementing strict security measures.

Psychological Impact: Effect on the public’s morale and confidence in national economic and political institutions.

Recovery. The development, coordination, and execution of service- and site-restoration plans for impacted communities and the reconstitution of government operations and services through individual, private sector, non-governmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents.

Response. Activities that address the short-term, direct effects of an incident. Includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk. A measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the SIPP, risk is the potential for loss, damage, or disruption to the State's CI/KR resulting from destruction, incapacitation, or exploitation during some future man-made or naturally occurring event.

Risk Management Framework. A planning methodology that outlines the process for setting security goals, identifying assets, assessing risks, prioritizing and implementing protective programs, and measuring effectiveness to produce a comprehensive, systematic, and rational assessment of national or sector risk that drives CI/KR risk-reduction activities.

Sector. A logical collection of assets that provides a common function to the economy, government, or society. The SIPP addresses 13 CI/KR sectors as defined by HSPD-7.

Sector Partnership Model. The framework for key security partners in the private sector, Federal agencies, States, Territories, local governments, and tribes to work together seamlessly in robust public private partnerships.

Sector-Specific Agency (SSA). Federal departments and agencies identified under HSPD-7 as responsible for the protection activities in specified CI/KR sectors.

Sector-Specific Plan (SSP). Augmenting plans that complement and extend the NIPP Base Plan and detail the application of the NIPP core processes specific to each CI/KR sector. SSPs are developed by the SSAs in coordination with other security partners.

Security Partner. A Federal, State, regional, Territorial, local, or Tribal government entity, private sector owners and operators of infrastructure, academic and professional entities, and certain not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation's CI/KR.

Steady State. In the context of the SIPP, steady state is the posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents.

System. In the context of the SIPP, a system is a collection of assets, resources, or elements that performs a process that provides infrastructure services to the Nation.

Terrorism. As defined in the Homeland Security Act of 2002, terrorism includes any activity that: (1) involves an act that is (a) is dangerous to human life or potentially destructive of critical infrastructure or key resources, and (b) a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (2) appears to be intended to (a) intimidate or coerce a civilian population, (b) influence the policy of a government by intimidation or coercion, or (c) affect the conduct of a government by mass destruction, assassination, or kidnapping.

Threat. An indication of possible violence, harm, or danger that includes both intent and capabilities. In the context of the SIPP, a threat is the likelihood that a particular target, or type of target, will suffer an attack or incident; for terrorist attack, threat likelihood is based on the analysis of the intent and capability of an adversary.

Vulnerability. A weakness in the design, implementation, or operation of an asset or system that can be exploited by an adversary or disrupted by a natural hazard.

References

Arizona Counter Terrorism Information Center. *GABRIEL*, December 2005.

Arizona Department of Homeland Security. *Arizona's Homeland Security Strategy*, October 2005.

Arizona Department of Homeland Security. State of Arizona 2006 Homeland Security Grant Program Enhancement Plan, March 2006.

U.S. Federal Bureau of Investigation. *Law Enforcement Online*, January 2003.

U.S. Office of Homeland Security. *Interim National Infrastructure Protection Plan*, Version 2.0, January 2006.

U.S. Office of Homeland Security. *National Preparedness Goal*, March 2005.

U.S. White House, Office of the Press Secretary. *Homeland Security Presidential Directive-7*, December 2003.

U.S. White House, Office of the Press Secretary. *Homeland Security Presidential* Directive-8, *December 2003.*